UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,198	07/01/2003	Carey Nachenberg	20423-07775	4107

34415 7590 11/14/2008
SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2437	
NOTIFICATION DATE	**DELIVERY MODE**
11/14/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptoc@fenwick.com
bhoffman@fenwick.com
aprice@fenwick.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *10/612,198*	**Applicant(s)** NACHENBERG ET AL.	
	Examiner Zachary A. Davis	**Art Unit** 2437	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 27 October 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) □ The period for reply expires ______months from the mailing date of the final rejection.

b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. □ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. □ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

(a)□ They raise new issues that would require further consideration and/or search (see NOTE below);

(b)□ They raise the issue of new matter (see NOTE below);

(c) □ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

(d)□ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. □ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. □ Applicant's reply has overcome the following rejection(s): _____.

6. □ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) □ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: *1,3,4,6-11,13-16,18-20 and 22-24*.
Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. □ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. □ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. □ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.

12. □ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. ☒ Other: See Continuation Sheet.

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's arguments are not persuasive. Regarding the rejections under 35 U.S.C. 103(a), and with specific reference to independent Claims 1, 16, and 20, Applicant argues that the combination of the admitted prior art, Ramarao, and Gruper does not teach or suggest the claimed invention. Applicant asserts that not only does Ramarao not explicitly disclose that commands are observed in real time before deriving the set of acceptable commands, as the Examiner acknowledged in the previous Office action (see page 6 of the final Office action mailed 25 August 2008, for example, in reference to Claim 1), but Ramarao also "explicitly requires" that the set of acceptable commands be specified a priori (see page 10 of the present response, citing Ramarao, paragraphs 0055 and 0056). The Examiner respectfully disagrees with this second assertion; the cited portion of Ramarao merely mentions the configuration file and that it can be configured to allow certain actions, for example. However, Ramarao does not specify, in this cited portion or elsewhere, exactly how the configuration file, which corresponds to the claimed set of acceptable commands, is generated or specified. There is certainly nothing in Ramarao that precludes the derivation of set of acceptable commands in real time, as taught by Gruper.

Applicant further argues that "the Examiner's rejection is based on a combination of alleged admitted prior art, Ramaro, and Gruper where a prior art database IDS is modified by Ramarao to allow previously-authorized commands having variable parameters, and then a training phase is run until a predetermined number of commands are received as taught by Gruper" (page 11 of the present response). However, this is a simplification and a distortion of the grounds of rejection as detailed in the previous Office action. While the admitted prior art (it is noted that although Applicant refers to this as "alleged admitted prior art", Applicant has not provided any evidence or reasoning to suggest that it was not, in fact, admitted as prior art, the "alleged" label notwithstanding) has correctly been characterized as relied upon for its disclosure of a database IDS, Ramarao was not relied upon for a teaching of allowing previously-authorized commands having variable parameters, but instead for more general disclosure of, for example, a method in which an intrusion detection system has derived a set of acceptable commands and groups commands into categories (again, see page 6 of the previous Office action, citing Ramarao, paragraphs 0056-0067, 0066, and 0032). Further, Gruper was relied upon not only for the teaching of the staistical analysis (for example, running the training phase until a predetermined number of operations is learned, see Gruper, column 2, lines 50-63), but also for the broader teaching of a security system having a learning mode in which commands are observed in order to compile an enforcement file of acceptable actions and commands are grouped into categories (see Gruper, column 5, lines 32-61, for example). In combination with the disclosure of Ramarao and the prior art of a database IDS incorporating access control principles based on acceptable commands, these broad teachings of Gruper are considered at least to suggest modifying such a database IDS to include real time training of the system (i.e. observing commands to determine acceptable actions, Gruper, column 5, lines 32-61). Again, there is nothing in Ramarao that requires that the set of commands (i.e. the described configuration file) to be determined beforehand, and nothing that precludes derivation of commands in real time, as taught by Gruper. In response to Applicant's argument that the resulting combination of admitted prior art, Ramarao, and Gruper would be "a DIDS in which acceptable commands are specified in advance, and then a training phase is ended when a predetermined number of acceptable commands is received" (page 11 of the present response), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Again, although Applicant asserts that Ramarao requires that the acceptable commands are "specified in advance", there is nothing in Ramarao that requires this. Further, Applicant's argument appears self-contradictory, because it refers to "ending a training phase" but also at least implicitly argues that no training phase would occur or be required because those commands were already specified in advance. In contrast, the Examiner submits that the teachings of Gruper would have suggested to one of ordinary skill in the art that the configuration file of Ramarao (corresponding to the claimed set of acceptable commands) could be derived through a real time observation, for the reasons previously asserted. Applicant also argues that the system "would not build any knowledge as to what commands are allowed since the authorized commands are already known" (page 11 of the present response, emphasis removed); however, Applicant provides no support for such a construction and merely alleges that "the combination would not derive the set of acceptable commands in real time" (page 12 of the present response). However, this alleged combination is mere conjecture, and does not appear to take into account the teachings of Gruper, which explicitly suggest training a system by observing and deriving acceptable commands in real time (again, column 5, lines 32-61). Applicant also alleges that the combination "changes the principle of operation" and "is inoperable for the purpose asserted" (pages 11-12 of the present response) but provides no evidence in support of such allegations, nor any explanation as to how the principle of operation is allegedly changed.

Continuation of 13. Other: The objection to the disclosure for informalities is withdrawn in light of the amendments to the specification. Applicant's cooperation is requested in correcting any other errors of which applicant may become aware in the specification.